THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

SIXTH EDITION

Editor
Alan Charles Raul

THE LAWREVIEWS

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

Sixth Edition

Reproduced with permission from Law Business Research Ltd
This article was first published in October 2019
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Alan Charles Raul

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Tommy Lawson

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anna Andreoli

SUBEDITOR
Charlotte Stretch

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC2A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-062-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ALLENS

ANJIE LAW FIRM

ASTREA

BOGSCH & PARTNERS LAW FIRM

BOMCHIL

BTS&PARTNERS

CLEMENS

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP. J.

MÁRQUEZ, BARRERA, CASTAÑEDA & RAMÍREZ

NNOVATION LLP

NOERR

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VUKINA & PARTNERS LTD

WALDER WYSS LTD

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

CONTENTS

Chapter 12

GERMANY

Olga Stepanova and Florian Groothuis[1]

I OVERVIEW

Germany has been and still is the forerunner on privacy and data protection law. In 1970, the German state of Hesse enacted the world's first Data Protection Act. The other states soon followed, and on 1 January 1978, the first German Federal Data Protection Act (BDSG) entered into force. These acts established basic principles of data protection, such as the requirement of a legal permission or the data subject's consent for any processing of personal data. In 1983, the German Federal Constitutional Court held that the individual even has a constitutional right to 'informational self-determination'. The background of this groundbreaking verdict was a census planned for the year 1983, which essentially focused on the census of the entire German population by the means of electronic data processing. The people of Germany were anything but pleased with this idea and – as a consequence – more than 1,600 complaints were filed at the Federal Constitutional Court against the census law that had been specifically adopted for the census by the German parliament. Finally, in December 1983, the German Federal Constitutional Court declared certain provisions of the Census Act to be unconstitutional.

Over time, the German Federal Data Protection Act was subsequently amended to meet the requirements of a society in which data processing has grown more important. Especially, digitalisation raised a lot of questions, which needed to be handled. Keeping this in mind, among others the legislator passed the German Telemedia Act (TMA) in 2007, which stipulated the duty to safeguard data protection during the operation of telemedia services. However, since data protection law and telemedia law got increasingly intersected by the internet, it was planned by the European legislator that the ePrivacy Regulation replacing the TMA would also come into force at the same time as the General Data Protection Regulation (GDPR). Whereas the GDPR has been applicable from 25 May 2018, the ePrivacy Regulation is still subject to negotiations at the European level and will probably be applicable in 2022. For this reason, the following text provides an overview of the current legal situation in Germany, presenting the changes and the challenges of a new era of data protection in connection with digitalisation.

1 Olga Stepanova is an associate and Florian Groothuis is a scientific researcher at Winheller Rechtsanwaltsgesellschaft mbH.

II THE YEAR IN REVIEW

The past year was characterised by compensating for the legal uncertainty caused by the new provisions of the GDPR. For this, the German data protection authorities published several working papers to give companies guidance on adjusting to the new data protection rules. Although the GDPR is directly applicable and does not have to be implemented into national law, it contains numerous 'opening clauses' so Member States can introduce additional national provisions to concretise provisions of the GDPR for specific issues (e.g., in connection with employees) within its legal framework.

The German legislator used this leeway and adopted a Data Protection Adaption Act which introduced in particular a new version of the BDSG and is applicable since the 25 May 2018. A second Data Protection Adaption Act is in the legislation process and focuses primarily on changes in area specific laws. Also it aims to modify the threshold from when data controllers and processors are obliged to designate a data protection officer from 10 to 20 persons being constantly employed in automated data processing activities.

Before the GDPR went into force, the mass media often reported about the high fines Data Protection Authorities (DPAs) are authorised to impose when infringements occur. In case of serious data protection violations the DPAs can indeed impose fines of up to €20 million or 4 per cent of annual global turnover, whichever is higher. However, the German DPAs acted rather restrained so far when sanctioning violations.

iii Basics

Although the GDPR maintains the main concepts of data protection as we knew them before, or amends details of them (e.g., data processing is still prohibited if not explicitly permitted by the data subject or a law, the legal bases for the transfer of personal data into non-EU countries or the obligation to designate a data protection officer), the new rules also bring some important changes. Small companies and non-profit organisations, in particular, are unsure about how to implement the GDPR, even after the regulation has been applicable for several months.

First and foremost, the GDPR extended its territorial scope, which means that non-European companies may also fall within its scope, making it the first worldwide data protection law due to globalisation. It applies to (1) all companies worldwide that target European markets and in this context process the personal data of European Union citizens (irrespective of where the processing takes place) and (2) those that process the data of European citizens in the context of their European establishments.

Since the GDPR has tightened the requirements for obtaining valid consent to process personal information, in practice, the relevance of the consent as legal basis has decreased and shifted to the legitimate interest of the data controller. Companies will therefore have to assess their processes to make sure they process personal data lawfully, and to review whether it is advisable to refrain from seeking consent but to switch to legal justification with fewer prerequisites and no possibility of being revoked at any time.

As a consequence, upon request of DPAs, companies have to provide prove that they fulfil their obligations under the GDPR. The authorities do not need to investigate and prove the infringements by themselves anymore. The GDPR also introduced mandatory privacy impact assessments (PIAs). It requires data controllers to conduct PIAs where privacy breach risks are high in order to minimise risks to data subjects. This means that before organisations can begin projects involving special categories of personal data, such as health, they will have to conduct a PIA and work with the data protection offices to ensure they are in compliance

with data protection laws as projects progress. For minimizing the uncertainty whether a PIA should be performed the German DPAs issued 'blacklists' that contain processing activities that always require a PIA.[2]

Additionally, the GDPR expanded liability beyond the data controllers. In the past, only data controllers were considered responsible for data processing activities, but the GDPR extended liability to all organisations that process personal data. The GDPR also covers any organisation that provides data processing services to the data controller, which means that even organisations that are purely service providers that work with personal data will need to comply with rules such as data minimisation.

To sum it up, the increase of obligations and fines are also likely to force previously idle organisations to rethink their positions.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person'. This definition applies to all personal data handled by electronic information and communication (telemedia) service providers.

However, all of these data are now subject to the GDPR, as the German Data Protection Conference presented a paper in March 2019, which states that Article 95 GDPR has to be interpreted in a way that the provisions of TMA governing the data protection shall not be applicable anymore. Following this opinion, there is no privileged handling for data collection via telemedia anymore, so the controllers must obey the strict rules prescribed by the GDPR from now on. That is why a lot of websites needed to amend not only their privacy policy, but also the cookie settings, so that i.e. for analysis cookies a consent under the strict rules of GDPR needs to be obtained.

ii General obligations for data controller

The privacy provisions of the GDPR address data controllers, namely entities that process personal data on their own behalf or commission others to do the same. Telemedia service providers as data controller may collect and use personal data only to the extent that the law specifically permits pursuant to Article 6 GDPR.

One relevant legal basis is still the consent according to Article 6 (1) (a) GDPR which may be given electronically, provided the data controller ensures that the user of the service declares his or her consent knowingly and unambiguously, the consent is recorded, the user may view his or her consent declaration at any time and the user may withdraw consent at any time with effect for the future. These principles accord with Article 7 GDPR, which requires consent to be based on the voluntary and informed decision of the data subject. Consent, however, is not always required.

As mentioned before, the focus to justify data processing activities has shifted towards the legitimate interest basis pursuant to Article 6 (1) (f) GDPR. For this, the data controller must perform a three-part test and identify the legitimate interest, explain the necessity of achieving it and balance the interest against the data subject's interests, rights and freedoms.

2 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_Verarbeitungsvorg%C3%A4nge%20-Muss-Liste%20Berlin%20%28002%29.pdf.

As long as the data subject would reasonably expect the respective processing activities and they have a minimal impact on the individual's privacy, no consent is needed. However, similar to the consent, the data subject has the right to object to processing activities based on the legitimate interest at any time according to Article 21 (1) GDPR. The important difference is that the data controller may continue its processing activities despite the data subject's objection when the data controller can demonstrate compelling legitimate grounds which override the individual's interests, rights and freedoms.

Moreover, personal data may only be collected for specified purposes the data controller has determined before the collection took place. They must not be used for secondary purposes that are incompatible with the collection purpose. When verifying the compatibility between the primary collection and the secondary processing purpose, the criteria named in Article 6 (4) GDPR are of paramount importance.

For ensuring the transparency of data processing activities the data controller is obliged according to Articles 13 and 14 GDPR, inter alia, to inform the user of the extent and purpose of the processing of personal data. Although the DPAs in Germany were hesitant in the beginning to allow a layered approach in providing the legally prescribed information, a change is emerging. Regarding video surveillance the German Data Protection Conference permits the distribution into essential information that must be provided onsite and other information that can be looked at online.[3] Single DPAs follow the layered approach as suggested by the European Data Protection Board in general.[4]

iii Technological innovation and privacy law

Cookies

Under data protection law, the use of cookies is only relevant if the information stored in the cookie is considered personal data. A cookie is a piece of text stored on a user's computer by his or her web browser. It may be used for authentication, storing site preferences, the identifier for a server-based session, shopping cart contents or anything else that may be accomplished through the storage of text data. The cookie is considered to be personal data if it contains data that allow the controller to identify the data subject.

However, before the GDPR entered into force, and as long as the relevant part of TMA was still applicable, cookies could have been placed in Germany as long as the user had the option to object (opt out). Now, there is no such privileged treatment anymore as the general requirements regarding a lawful data processing are applicable for cookies too. The only question not answered so far by the European Court of Justice (ECJ) is whether the use of cookies must inevitably be based on the data subject's consent (Article 6(1)(a) GDPR) or is it sufficient when the controller states that this use is necessary for the purposes of his legitimate interest (Article 6(1)(f) GDPR). In any case, according to the German Data Protection Conference, prior consent is required for the use of tracking mechanisms, which monitor the behaviour of data subjects on the internet and create user profiles. Thus, an

3 DSK, Kurzpapier Nr. 15, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_15.pdf.

4 LDA Bayer, 8. Tätigkeitsbericht, https://www.lda.bayern.de/media/baylda_report_08.pdf#page=45; EDPB, Working Paper 260, https://datenschutz-hamburg.de/assets/pdf/wp260rev01_en.pdf.

informed consent within the meaning of the GDPR is required in the form of a declaration or other clearly confirmatory action taken prior to data processing (i.e., before cookies are placed on the user's device).[5]

The reason for this discussion and the legal uncertainty is derived from the fact that the ePrivacy Regulation did not enter into force on time and has not even been passed. So far, it may be advisable to fulfil all the requirements of the GDPR, which means that consent has to be sought before tracking the user.

Social media

Social media becomes more popular each day as the number of users grows. The same applies to the opportunities and smart solutions offered by using these media. Most social media platforms are free of charge. Users pay with their personal data, even though many of them are not even aware of this fact. That is why the European legislator stipulated in the principles of processing in Article 5 GDPR that processing has to be transparent and the controller shall be responsible for obeying this principle.

An important part of the transparency principle is providing understandable information about the division of roles when involved parties are processing personal data, as the ECJ on Facebook fanpages has shown (ECJ, 5 June 2018 – C-210/16). In this case the ECJ stated that the fanpage operator and Facebook are acting as joint controllers. Although the main responsibility for data collection lies with Facebook, it is theoretically possible for the page operators to place cookies on the visitor's device, even if the visitor does not have a Facebook account. According to the ECJ, this in addition to the fact that fanpage operators receive the visitor's user data (even if anonymised) and can use these for parameterisation lead to joint responsibility of the site operators. This is particularly because of the fact that the collection of this data cannot (yet) be deactivated. Until Facebook grants this option to its users, the common fanpage operator remains jointly responsible for the collection of user data. Even the ECJ takes account of the significant imbalance in the use of data between Facebook and the operators of the respective fan page insofar as the degree of responsibility can be assessed differently in individual cases; however, in the court's opinion, Facebook and the fanpage operators are still joint controllers.

Facebook reacted and published a Page Insights Controller Addendum to fulfil the requirements established by the ECJ regarding joint controllership. Nevertheless, the German Data Protection Conference found these adjustments insufficient and therefore in violation of the GDPR. In particular, Facebook grants itself the sole decision-making power in respect of the processing of insights data and this is in conflict with the joint controllership pursuant to Article 26 GDPR. Furthermore, Facebook does not describe the processing activities regarding the fanpage in a transparent way.[6]

While the ECJ confirmed its findings in respect of the joint controllership in the Jehovah's Witnesses decision (ECJ, 10 July 2018 – C-25/17), they will be relevant in another dispute before the ECJ involving Facebook. The Düsseldorf Higher Regional Court has asked the ECJ, inter alia, whether a German online retailer that includes the 'Facebook Like' button

5 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

6 DSK, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook Fanpages, https://www.datenschutzkonferenz-online.de/media/dskb/20190405_positionierung_facebook_fanpages.pdf.

on its website is a joint controller alongside Facebook. The Advocate General confirmed joint controllership and set a low threshold for assuming joint controllership (Opinion of Advocate General Bobek, 19 December 2018 – C-40/17).

However, this decision and the German Federal Court's decision regarding the obligation of Facebook to provide heirs with access to the digital postbox of the decedent (BGH, 12 July 2018 – III ZR 183/17), clearly show that social media is now being regulated more strictly.

IV INTERNATIONAL DATA TRANSFER AND DATA LOCALISATION

The international transfer of personal data is regulated within the framework of Articles 44–50 GDPR. There is a general distinction between transfers within the EU and EEA or to one of the 'trusted countries' for which the European Commission has confirmed by means of an 'adequacy decision' that these countries ensure an appropriate level of data protection on the one hand and transfers to third countries on the other. For an international data transfer to be lawful, it must comply not only with the aforementioned articles, but must also be in compliance with the general provisions pertaining to the legality of processing operations involving personal data.

i Data transfer within the EU or EEA

In contrast to the former legal situation, the GDPR does not explicitly stipulate that there is no difference between transfers within Germany or within EU or EEA. Therefore, the only distinction is made between domestic transfers (within the EU or EEA) and those outside the EU or EEA.

ii Data transfer to countries outside the EU or EEA

If a private entity intends to transfer personal data internationally to another entity located outside the area of the EU or EEA (a third country), Article 44 GDPR specifies the requirements for such a transfer. In this respect, personal data shall not be transferred when the data subject has a legitimate interest in being excluded from the transfer. A legitimate interest is assumed when an adequate level of data protection cannot be guaranteed in the country to which the data are transferred.

An adequate level of data protection exists in certain third countries that have been identified by the European Commission. These are Andorra, Argentina, Guernsey, the Isle of Man, Canada (limited), the Faroe Islands, Israel (limited), Guernsey, Jersey, New Zealand, Japan, Switzerland and Uruguay. Any transfer of personal data to these countries will only have to satisfy the requirements of domestic data transfers.

Uncertainty currently surrounds data transfers to the United States. After the European Court of Justice declared the Safe Harbour principles of the Commission invalid, the Commission enacted the EU–US Privacy Shield. Under the protection of the new principles of the Privacy Shield the United States is found to have an adequate level of data protection. But the Privacy Shield itself is again the target of a great deal of criticism. There are currently several complaints pending against the Privacy Shield at the European Court of Justice.

Data transfers to any other non-EU country may be justified by the derogation rules of Article 49 GDPR. Accordingly, the international transfer of personal data is admissible if:

a the data subject has given his or her consent;

b the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;

c the transfer is necessary for the conclusion or performance of a contract that has been or is to be concluded in the interest of the data subject between the controller and a third party;

d the transfer is necessary for important reasons of public interest;

e the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims;

f the transfer is necessary to protect the vital interests of the data subject; or

g the transfer is made from a register that is intended to provide information to the public, and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law are fulfilled in the particular case.

The most relevant grounds are those given in (b), namely if the transfer is necessary to perform a contract between the data subject and the controller. This includes international monetary transactions and distance-selling contracts as well as employment contracts. All transfers in this respect have to be essential for the purposes of the contract.

Any consent within the meaning of (a) will only be valid if the data subject was informed about the risks that are involved in data transfers to countries that do not have an adequate standard of data protection. In addition, the consent has to be based on the data subject's free will; this may be difficult if employee data are involved.

If none of the aforementioned exceptions applies, the transfer of personal data to third countries with an inadequate level of data protection is nonetheless possible if, among other requirements, the competent supervisory authority authorises the transfer. Such an authorisation will only be granted when the companies involved adduce adequate safeguarding measures to compensate for a generally inadequate standard of data protection, see Article 49(1)2 GDPR. However, the primary safeguarding measures are the use of standard contractual clauses issued by the European Commission and the establishment of binding corporate rules.

iii Brexit

The free flow of data between EU Member States and the United Kingdom (UK) depends whether the UK and the EU can reach a deal that covers data protection before the UK leaves the EU. Since the Commission has declined to start the process of assessing the UK's level of data protection and declaring it for adequate, a 'hard' Brexit would have a severe impact on the unhindered data exchange between the EU and the UK. In such scenario, the UK would be treated from a data protection point of view as third country equivalent to India. Therefore, personal data could only be transferred to the UK when companies have implemented the above-mentioned safeguards, namely standard contractual clauses and binding corporate rules.

V PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Germany has a Federal Data Protection Agency and 16 state data protection agencies. These often act in concert when making recommendations on how customers can navigate safely through the internet. In addition, German experts often discuss the data protection problems that arise from the widespread collection of data by search engines and social media, and the use of these data to profile the data subject for commercial purposes.

The state data protection agencies are authorised to supervise the data privacy compliance of state entities, as well as all non-public entities whose principal place of business is established in the particular state and that are not subject to the exclusive jurisdiction of the federal supervisory authority. In states that have enacted a freedom of information act, the state supervisory authorities are typically also charged with supervising the act's application by state entities.

The heads of the supervisory authorities are typically appointed by the federal and state parliaments respectively, and are required to report to their respective parliaments.

ii Material enforcement cases

One of the most discussed amendments specified by the GDPR and the new BDSG is the dramatic increase of the framework for fines. Before, the fines for data protection breaches were up to €300,000 per breach. Now, fines are up to €20 million or, in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher. This massive increase is directly addressed to Big Data companies, which are often suspected of processing data in an unlawful way, and can be used as sharp sword to ensure conformity with GDPR. Especially the dynamic and the dependency on the turnover aims to achieve a deterrent effect even on the most be wealthiest companies worldwide.

However, fines amounting to millions, as feared by companies, have not yet been imposed by the German DPAs. The DPA of the federal state of Baden-Württemberg imposed a fine of €80,000 because health data were accidently published on the internet. In another case a bank was fined €50,000 by the DPA of the federal state of Berlin for processing personal data of former clients without legal grounds.

Mostly infringements are caused by insufficient internal compliance activities of companies where the responsible management carelessly contravened the high standards of data protection law (e.g., through video surveillance or keylogging). Another source of data protection breaches is the lack of employee training, which shall ensure that everybody in the company has the necessary knowledge to handle personal data in a lawful way.

iii Information obligations in context of private litigation

The GDPR obliges the data controller to provide the data subject with certain information about the data processing (see Articles 13 and 14 GDPR). It must inform the data subject about the identity and the contact details of the controller, the contact details of the data protection officer, if applicable, the purposes of the processing and its legal basis, the source of the data, where applicable, to whom they are disclosed, the duration of processing and the retention policy. Additionally, the data subject must be informed regarding all his or her rights granted by the GDPR. In detail, this notification has to contain information concerning the right to information, right to rectification, right to be forgotten, right to restriction of

processing, right to data portability, right to object and the right to lodge a complaint with a supervisory authority. This clearly shows that the data subject is being given numerous rights, but also that the controller will have to invest more effort in satisfying the requests in a proper way, which is a question of time and expense.

The privacy rights and remedies of telemedia users are governed to a large extent by Article 77 GDPR (the right to lodge a complaint with a supervisory authority) and Article 82 GDPR (the right to compensation). Data subjects may enforce their rights through the judicial remedies provided in civil law. Injunctive relief as well as damages can be claimed. In particular, damages for pain and suffering from data protection violations can be claimed under civil law.

In Germany, the DPAs are not necessarily involved in enforcing the rights of individual data subjects. Instead, complaints against domestic controllers can first be lodged with the company's in-house data protection officer.

However, in the event of unsatisfactory contact with the company data protection officer, the supervisory authority and the civil courts can, of course, be called upon.

VI CONSIDERATIONS FOR FOREIGN ORGANISATIONS

As data protection gradually becomes a question of technical measures, especially cybersecurity, Article 32 GDPR determines that pseudonymisation and encryption has to be applied to lower the risk of damaging the data subject in case of data breaches.

The implementation of such and similar technical measures may safeguard the controller from notifying a data breach to the relevant authority as the risk to the rights and freedoms of natural persons had been reduced from the start. As Article 33(1) GDPR stipulates that data breaches, where feasible, shall be notified by the controller to the supervising authority within 72 hours. Therefore, controllers have to implement an effective data protection management system to be able to meet the deadline. Otherwise, a violation of this provision alone can be punished with a fine of up to €10 million or in the case of an undertaking, up to 2 per cent of the total worldwide annual turnover of the preceding financial year.

VII OUTLOOK

The GDPR is still not fully understood and often only can be understood by a teleological interpretation. In Germany, there are 16 DPAs that follow slightly different interpretations of the GDPR legislation. This complicates advising in privacy matters. Therefore, it will be interesting to see how the new laws will be interpreted by German and European courts. Furthermore, we are looking forward to seeing the report of the Commission on the evaluation and review of the GDPR that is due by 25 May 2020 and what impact the GDPR will have on companies until then, especially on social media operators.

Appendix 1

ABOUT THE AUTHORS

OLGA STEPANOVA

Winheller Attorneys At Law & Tax Advisors

Olga Stepanova heads the IP/IT department at Winheller Attorneys at Law & Tax Advisors, where she advises German and international companies and non-profit organisations on issues of data protection, IT law and intellectual property.

FLORIAN GROOTHUIS

Winheller Attorneys At Law & Tax Advisors

Florian Groothuis is scientific researcher at the IP/IT department at Winheller Attorneys at Law & Tax Advisors and is specialised in data protection law and IT related legal matters.

WINHELLER ATTORNEYS AT LAW & TAX ADVISORS

Tower 185
Friedrich-Ebert-Anlage 35–37
60327 Frankfurt
Germany
Tel: +49 69 76 75 77 80
Fax: +49 69 76 75 77 810
info@winheller.com
www.winheller.com/en

an LBR business

ISBN 978-1-83862-062-2